January 2015

Holly Hill Infant & Nursery School
Data Protection Policy

1 The school will comply with:

1.1 The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
1.2 Birmingham LA advice and guidance (www.bgfl.org/data)
1.3 Information and guidance displayed on the Information Commissioner's website (www.ico.gov.uk).
1.4 Guidance from Becta (http://schools.becta.org.uk).

2 This policy should be used in conjunction with the school's Internet Use Policy.

3 Data Gathering

3.1 All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
3.2 Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made, through the issuing of a Privacy Notice. (Pupils – appendix (i), Staff – appendix (ii).)
3.3 Data Protection statements will be included on any forms that are used to collect personal data.

4 Data Storage

4.1 Personal data ('Protected') will be stored in a secure and safe manner.
4.2 Electronic data will be protected by standard password and firewall systems operated by the school, and by encryption. Personal data will only be stored on computers, laptops and USB memory devices which are the property of the school and have been protected by encryption software.
4.3 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
4.4 Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
4.5 Particular attention will be paid to the need for security of sensitive personal data ('Restricted') which should not be removed from the school premises. .
4.6 'Confidential' data will be stored in locked filing cabinets or the school safe.

5 Protective Marking

5.1 Electronic documents will be marked in the footer or header. Printed paper documents will be stamped or marked in ink. The terms used will be consistent with the Government Marking Scheme:

- Not Protectively Marked
- Protect (personal data such as, address, ethnicity, etc)
- Restricted (sensitive data such as SEN, IEP, Medical)
- Confidential (such as Child Protection)

See appendix (iii) 'working out the appropriate Protective Marking for data'.

6 Data Transfer

- All electronic data that is marked 'Protect, Restricted or Confidential' should be encrypted before transfer.
- Removable media (USB pen drives, CDs, portable drives) need to be encrypted before being taken or sent out of school.
- When pupils transfer to another school paper records will be sent by Special Delivery.
- Third parties should be asked how they will protect sensitive information once it has been passed to them.

7 Data Retention and Disposal

7.1 Personal data should not be retained for longer than necessary.
7.2 Data will be retained according to the Records Management Society guidelines (see Retention Schedule at www.rms-gb.org.uk/resources/848
7.3 Disposal of data: Documents marked protected, restricted or confidential should be shredded when no longer needed.
7.4 Confidential waste is shredded onsite by an accredited company which provides certificates of disposal.
7.5 When a member of staff ceases to work at the school, documents and data storage devices must be returned to the school.
7.6 Personal data should be removed from IT equipment before disposal.
7.7 IT equipment is recycled by an accredited company which provides certificates of secure removal of data.

8 Data Checking

8.1 The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.
8.2 Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

9 Data Disclosures

9.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

9.2 When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

9.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

9.4 Requests from parents or children for printed lists of the names of Children in particular classes, which are frequently sought at Christmas, should politely be refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem.)

9.5 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

9.6 Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

9.7 Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data. This form is the agreed procedure between Birmingham City Council and West Midlands Police.

9.8 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate. (Disclosure file kept in the school office)

10 Subject Access Requests

10.1 If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.

10.2 Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

11 Staff Training

11.1 This policy will be included on the school's BGFLplus Page accessible to all staff.

11.2 Staff will receive regular data protection training.

12. Data Security Incidents

Breeches to this policy and any suspected loss of data should be reported to the school's SIRO (Senior Information Risk Owner), Mrs Christine Parker.

13. Off Site Working

Staff are expected to take all reasonable steps to protect school data whilst it is being processed away from the school in accordance with this policy.

Appendix (i)

January 2015

PRIVACY NOTICE for pupils in schools, early years settings, alternative provision and pupil referral units.

Privacy Notice – Data Protection Act 1998

We, Holly Hill Church School are the Data Controller for the purposes of the Data Protection Act. We collect information from you, and may receive information about you from your previous school. We hold this personal data and use it to:

- support your teaching and learning;
- monitor and report on your progress;
- provide appropriate pastoral care, and
- assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information [A], characteristics such as ethnic group, special educational needs and any relevant medical information.

We will not give information about you to anyone outside the school without your consent unless the law and our rules permit it.
We are required by law to pass some of your information to the Local Authority (LA), and the Department for Children, Schools and Families (DCSF).

If you want to see a copy of the information we hold and share about you then please contact Mrs Ingleby.

If you require more information about how the LA and/or DCSF store and use this data please go to the following websites:

- www.birmingham.gov.uk and search Data
- www.teachernet.gov.uk and search Data Protection

If you are unable to access these websites, please contact the LA or the DCSF as follows:

Steve Cullen
Information Governance Manager
Children, Young People and Families Directorate
Birmingham City Council
Martineau Centre
Balden Road
Birmingham B32 2EH
Tel: 0121 464 4591

[A] Attendance information is not collected for pupils under 5 at Early Years Settings or Maintained Schools

- Public Communications Unit
  Department for Children, Schools and Families
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  website: www.dcsf.gov.uk
  email: info@dcsf.gsi.gov.uk
  tel: 0870 000 2288.

Appendix (ii)

PRIVACY NOTICE for the school workforce employed or otherwise engaged to work at a school or the Local Authority

Privacy Notice - Data Protection Act 1998

We, Holly Hill Church School, are the Data Controller for the purposes of the Data Protection Act.

Personal data is held by the school about those employed or otherwise engaged to work at the school or LA. This is to assist in the smooth running of the school and/or enable individuals to be paid. This personal data includes some or all of the following: identifiers such as name and National Insurance Number; characteristics such as ethnic group; employment contract and remuneration details; post "A" level qualifications; and absence information.

The collection of this information will benefit both national and local users by:

- improving the management of school workforce data across the sector;
- enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- informing the development of recruitment and retention policies;
- allowing better financial modeling and planning;
- enabling ethnicity and disability monitoring;
- supporting the work of the School Teacher Review Board and the School Support Staff Negotiating Body.

We are required to pass on some of this data to:

- the LA
- the Department for Children, Schools and Families (DCSF).

If you require more information about how the LA and/or DCSF store and use this data please go to the following websites:

- www.birmingham.gov.uk and search Data
- www.teachernet.gov.uk and search Data

If you are unable to access these websites, please contact the LA or the DCSF as follows:

- Steve Cullen - Information Governance Manager, Martineau Education Centre, Tele No: 464 4591

- Public Communications Unit
  Department for Children, Schools and Families
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  website: www.dcsf.gov.uk
  email: info@dcsf.gsi.gov.uk

tel: 0870 000 2288.

We will not give information about you to anyone outside the school or LA without your consent unless the law and our rules allow us to.

Working out the appropriate Protective Marking for data

Educational organisations should use information risk management to help them look after the security of personal data, sensitive personal data and data that is critical to the organisation.

Protective marking is designed to identify – and protect – data that falls into these three categories. The simplified process described below will help organisations to choose the appropriate protective markings by carrying out the first few stages of an information risk assessment.

Step 1

Imagine a potential security breach, and consider:

1. Will it affect any member of the public?
2. Will someone lose more than £100?
3. Will it cause any kind of criminal case to fail?
4. Is there a risk of discomfort to someone?
5. Is anyone's personal safety at risk?
6. Will it embarrass anyone?

If you answered **no** to **all** the questions, a document can be labelled as **NOT PROTECTIVELY MARKED**. This shows everyone that you have assessed it. If you answered **yes** to any of the questions, the document requires a higher level of protective marking.

Step 2

Imagine the *same* potential security breach as above, and consider:

1. Will it affect many members of the public and need extra resources locally to manage it?
2. Will an individual or small trader lose £1000 to £10,000?
3. Will a serious criminal case or prosecution fail?
4. Is someone's personal safety at a moderate risk?
5. Will someone lose his or her reputation?
6. Will a large company or organisation lose £100,000 to £1,000,000?

If you have answered **yes** to **any** of the above questions, mark your document as **RESTRICTED**. However, if you think that the potential impact *exceeds* that stated in the question (for example, someone's personal safety is at high risk) mark your document as **CONFIDENTIAL**.

Step 3

Mark all documents that **do not fit** NOT PROTECTIVELY MARKED **or** RESTRICTED as **PROTECT**. Where there is concern that a document *might* require a higher level of protection, organisations should err on the side of caution.

In general, most of your documents and data should be either NOT PROTECTIVELY MARKED or PROTECT.

Information risk actions form

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk